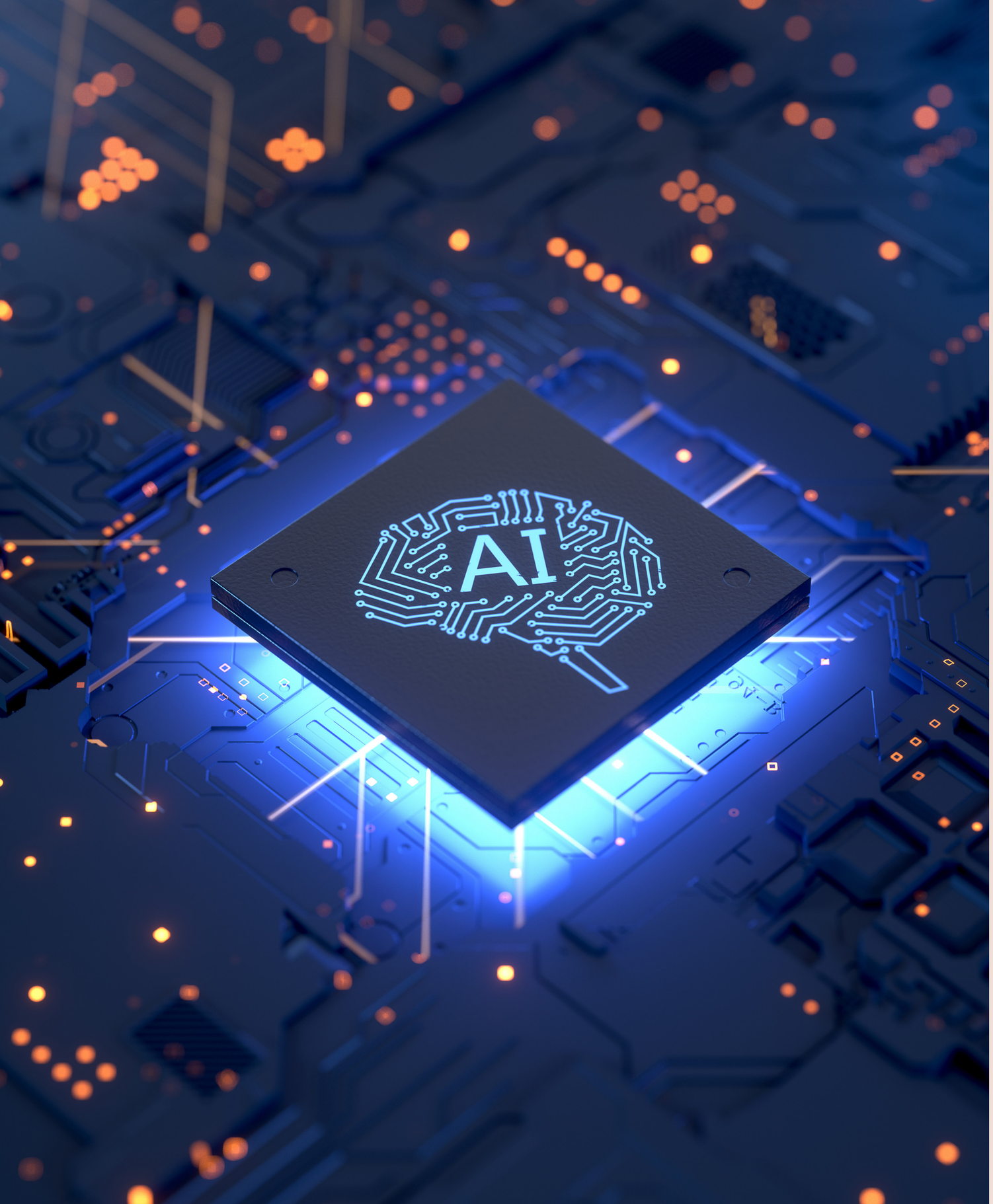


PART 21

NAVIGATING THE NEW FRONTIER: CONTRACTUAL DYNAMICS FOR AI CONTRACTS

YENİ SINIRLARI KEŞFETMEK: YAPAY ZEKA SÖZLEŞMELERİNİN DİNAMİKLERİ

F. GÖZDE KARDEŞ

PART 21

ABSTRACT | ÖZET

This article explores the impact of artificial intelligence (AI), especially generative artificial intelligence (GenAI) on traditional software arrangements; in this article, we'll guide you through certain key considerations that should be taken into account when negotiating GenAI agreements and the allocation of risks associated with GenAI in a practical, hands-on manner.

Bu makale, yapay zekanın, özellikle üretken yapay zekanın, geleneksel yazılım anlaşmaları üzerindeki değişim etkisini incelemektedir; bu makalede, üretken yapay zeka sözleşmeleri müzakere edilirken dikkate alınması gereken temel hususları ve üretken yapay zeka ile ilişkili risklerin pratik bir yaklaşımla ilgililer arasında nasıl paylaştırılabileceğini ele alacağız.

KEYWORDS | ANAHTAR KELİMELER

Artificial Intelligence, Generative AI, Large Language Models, AI Tools Supply Contracts, AI as a Service Contracts, AI Tool Development Contracts.

Yapay Zeka, Üretken Yapay Zeka, Büyük Dil Modelleri, Yapay Zeka Araçları Tedarik Sözleşmeleri, Yapay Zeka Hizmet Sözleşmeleri, Yapay Zeka Aracı Geliştirme Sözleşmeleri.

I. INTRODUCTION

I. GİRİŞ

As AI evolves, understanding how to navigate contractual arrangements and distribute risks associated with AI can be daunting. The rapid and exponential advancement of AI technology introduces a new dimension of complexity and opportunity into software contracts.

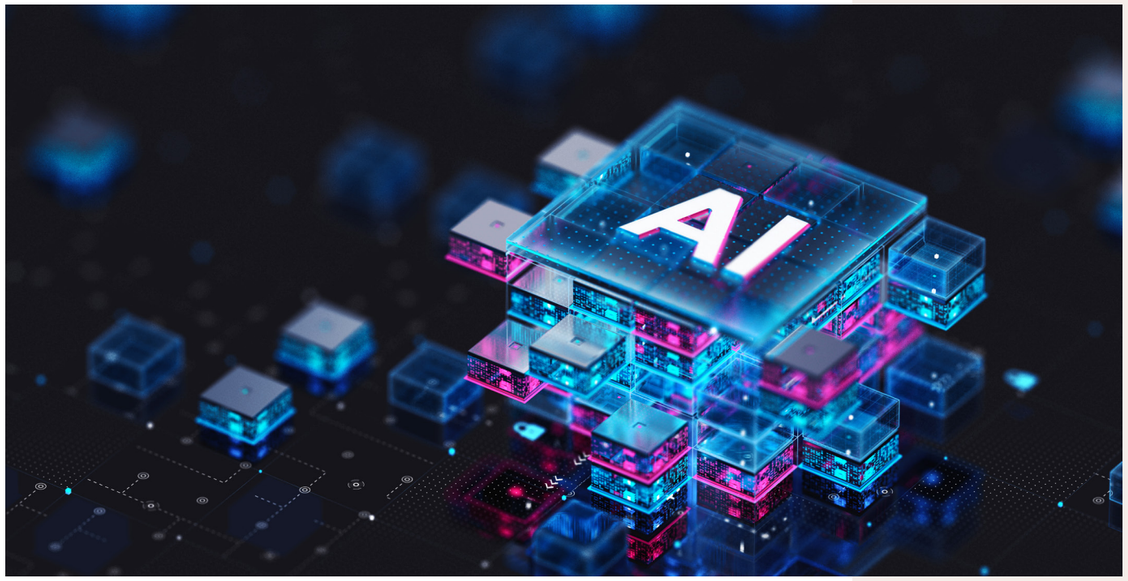
Yapay zeka geliştikçe, yapay zeka ile ilişkili sözleşme düzenlemelerini ve taraflar arasındaki risk paylaşımını anlamak zorlayıcı olabilir. Yapay zeka teknolojisinin hızla ve katlanarak ilerlemesi, yazılım sözleşmelerine hem karmaşıklık hem de fırsat anlamında yeni bir boyut katmaktadır.

While, AI, especially GenAI becomes increasingly prevalent, new contract types have emerged, such as those for AI tools supply contracts, provision of AI as a service, and AI tool development contract.

Yapay zeka, özellikle üretken yapay zeka, giderek daha yaygın hale geldikçe, yapay zeka araçları tedarik sözleşmeleri, yapay zeka hizmeti sağlama sözleşmeleri ve yapay zeka aracı geliştirme sözleşmeleri gibi yeni sözleşme tipleri ortaya çıkmıştır.

In traditional software contracts, where suppliers either develop or supply software solutions (either as a service or as a product), critical factors during contract negotiations include exclusivity, liability, warranties, service levels, intellectual property, third-party software, personnel, protection of customer data, security, and indemnities. The emerging contract types, however, introduce distinct challenges, necessitating updates to traditional contract clauses and the inclusion of new terms. Examples include provisions related to restrictions on using customer data for training, error management (noting that the tool may be offered on an "as-is" basis without guarantees of continuous or

Tedarikçilerin yazılım çözümleri (hizmet veya ürün olarak) geliştirdiği veya tedarik ettiği geleneksel yazılım sözleşmelerinde, sözleşme müzakereleri sırasında dikkate alınan kritik hususlar arasında münhasırlık, sorumluluk, garantiler, hizmet seviyeleri, fikri mülkiyet, üçüncü taraf yazılımları, personele ilişkin konular, müşteri verilerinin korunması, güvenlik ve tazminatlar yer almaktadır. Bununla birlikte, yeni ortaya çıkan sözleşme tipleri, geleneksel sözleşme maddelerinin güncellenmesini ve yeni şartların dahil edilmesini gerektiren farklı zorluklar ortaya koymaktadır. Örnekler arasında, müşteri verilerinin eğitim için kullanılmasına ilişkin kısıtlamalar, hata



error-free operation), measures to combat bias and related liability, and requirements for record keeping and auditing of the AI tool.

yönetimi (yapay zeka aracının sürekli veya hatasız çalışma garantisi olmaksızın "olduğu gibi" sunulması), yapay zekanın önyargılı yanıtlar vermesi ve bundan doğan sorumlulukla mücadele için alınabilecek önlemler ve yapay zeka aracının kayıt tutma ve denetleme gereklilikleri ile ilgili hükümler yer almaktadır.

AI contracting becomes even more challenging where the supplier does not develop or supply AI tools "as such," but rather uses AI tools to develop software, which is then supplied to customers.

Yapay zeka sözleşmeleri, tedarikçinin doğrudan yapay zeka aracı geliştirmediği veya tedarik etmediği, ancak yazılım geliştirmek için yapay zeka araçlarını kullandığı ve daha sonra bunu müşterilere sunduğu durumlarda daha da karmaşık hale gelmektedir.

II. KEY CONSIDERATIONS ON AI TOOLS, USE OF AI TOOLS AS PART OF SERVICES AND AI TOOLS DEVELOPMENT CONTRACTS PROVISIONS

II. YAPAY ZEKA ARAÇLARI, HİZMETLERİN BİR PARÇASI OLARAK YAPAY ZEKA ARAÇLARININ KULLANIMI VE YAPAY ZEKA ARAÇ GELİŞTİRME SÖZLEŞMELERİNDE DİKKATE ALINMASI GEREKEN ÖNEMLİ HUSUSLAR

In today's dynamic business landscape, companies are now looking to their service providers/ suppliers to design and explore AI use cases to streamline operations, enable more efficient capacity and less duplicative

Günümüzün dinamik iş ortamında, şirketler artık operasyonlarını optimize etmek, daha verimli kapasite ve daha az tekrar eden süreçler benimsemek, maliyetlerini azaltmak, özel uzmanlığa erişmek ve nihayetinde ra-

PART 21

resources, cut costs, access specialized expertise, and finally to get out ahead of competitors. While senior managements are rushing to leverage AI (particularly GenAI), compliance and legal teams are rushing to understand the risk implications of AI usage, from confidentiality and intellectual property issues to quality and performance concerns and put guardrails in place to ensure "responsible" use of AI.

As companies are understanding the risks and implications of AI, developing broad and strict AI policies may be the best defense, but as service providers/ suppliers demonstrate safe use cases the requirements may soften. Regarding concerns of security in the cloud, we are seeing, for instance, some providers/ suppliers looking ahead and proactively offering terms that demonstrate how they use AI in a responsible manner attempting to allay at least some concerns.

Although the specific implementation of any of these clauses will of course be subject to negotiations between the supplier/ developer and the customer and depend on the exact nature and subject matter of the contract, on applicable laws and on the priorities, business model and business strategy of the contracting parties, in the following sections, we delve into key concepts pertinent to contracts involving the supply of AI tools, provision of AI-as-a-service, and the development of AI tools. We will also try to illuminate essential considerations for each

kiplerinin önüne geçmek için hizmet sağlayıcılarından/ tedarikçilerinden yapay zeka kullanım senaryoları tasarlamalarını ve ortaya koymalarını beklemektedirler. Üst düzey yöneticiler yapay zekadan (özellikle üretken yapay zekadan) yararlanmak için acele ederken, uyum ve hukuk ekipleri de, gizlilik ve fikri mülkiyet sorunlarından kalite ve performans endişelerine kadar yapay zeka kullanımının risk sonuçlarını anlamak ve yapay zekanın "sorumlu" kullanımını sağlamak için gereken önlemleri bir an evvel devreye sokmak için acele etmektedir.

Şirketler, yapay zeka ile ilgili riskleri ve etkilerini anladıkça, bunlara karşı en iyi korunma yöntemi olarak geniş kapsamlı ve sıkı yapay zeka politikaları geliştirmektelerse de, hizmet sağlayıcılar/ tedarikçiler güvenli kullanım senaryoları ortaya koydukça, bu sıkı politikaların gereklilikleri yumuşamaktadır. Örneğin bulut ortamı temelli teknolojiler kullanan bazı sağlayıcıların/ tedarikçilerin, müşterilerinin güvenlik kaygıları konusunda proaktif davrandıklarını ve yapay zekayı sorumlu bir şekilde nasıl kullandıklarını gösteren düzenlemeler yaparak en azından bazı endişeleri gidermeye çalıştıklarını görüyoruz.

Makalemizde, yapay zeka araçlarının tedarik edilmesi, yapay zekanın bir hizmet olarak sağlanması ve yapay zeka araçlarının geliştirilmesiyle ilgili sözleşmelere yönelik önemli kavramlara daha yakından bakacağız. İşaret edeceğimiz hükümlerden herhangi birinin spesifik uygulaması, elbette ki tedarikçi/ ge-

agreement type, including the nuances, negotiation points, and motivations of the parties involved.

A. Defining "Artificial Intelligence"

The use cases for AI applications are increasing exponentially—from generative AI tools to analytical and reporting AI tools such as transaction monitoring and risk management visualization. The parties, particularly customers, may prefer to avoid a narrow definition of AI; a broad contractual definition would capture any algorithmic, interpretive, machine learning, or other AI processes. However, in doing so, certain other requirements such as disclosure and quality checks may be challenging or at least require diligence and work, i.e., resources and time.

B. Disclosure & Due Diligence of AI Use

Depending on the definition of AI, the complexities of determining where and how GenAI is currently being used by the service provider (that is to say, how operational decisions and processes utilize or are based on the outputs of AI) and whether there is appropriate disclosure and understanding of such use may be an issue. There are many reasons why a customer must understand where and how AI is used in its services and environments. Particularly where the AI processes train large language models (LLMs) using company data or a company's customer data, a service provider may be contractually obligated to keep the customer generally informed of AI usage as part of its services.

A customer may also seek a right to receive specific information on the use of AI as part of the services, on request. A service provider might counterbalance such a right with protecting its commercially sensitive business information and the confidential information of other customers whose data sets are used to train the AI tool or that benefit from the AI tool.

liştirici ve müşteri arasındaki müzakerelere, sözleşmenin hukuki niteliğine, konusuna, uygulanacak hukuka, tarafların önceliklerine, iş modeline ve iş stratejisine bağlı olacaksa da, her sözleşme tipi için nüanslarıyla birlikte temel hususları, müzakere noktalarını ve tarafların motivasyonlarını aydınlatmaya çalışacağız.

A. Yapay Zekanın Tanımlanması

Üretken yapay zeka araçlarından, işlem izleme ve risk yönetimi görselleştirme gibi analitik ve raporlama yapay zeka araçlarına kadar, yapay zeka uygulamaları için kullanım senaryoları katlanarak artmaktadır. Taraflar, özellikle müşteriler, yapay zeka için dar bir tanımdan kaçınmayı tercih edebilirler; zira geniş bir sözleşmesel tanım, algoritmik yapay zeka, yorumlayıcı yapay zeka, makine öğrenimi süreci veya diğer yapay zeka süreçlerini de kapsayacaktır. Ancak, uygun tanımlama yapılırken, ifşa gerekleri ve kalite kontrolleri gibi diğer gereksinimler zorlayıcı olabilir veya en azından hassas ve özenli bir çalışma, dolayısıyla ilave kaynak ve zaman, gerektirebilir.

B. Yapay Zeka Kullanımının Açıklanması & Durum Tespiti

Yapay zekanın tanımına bağlı olarak, hizmet sağlayıcının güncel durumda üretken yapay zekayı nerede ve nasıl kullandığını (yani, operasyonel kararların ve süreçlerin yapay zekanın çıktıları üzerinde nasıl şekillendiğini) belirlemek ve bu kullanımın uygun şekilde açıklanıp anlaşılmasını sağlamak karmaşık bir konu olabilir. Bir müşterinin, hizmetlerinde ve iş süreçlerinde yapay zekanın nerede ve nasıl kullanıldığını anlaması birçok nedenle önemlidir. Özellikle yapay zeka süreçlerinin şirket verilerini veya bir şirketin müşteri verilerini kullanarak büyük dil modellerini (LLM'ler) eğittiği durumlarda, hizmet sağlayıcı müşteriyi hizmetlerinin bir parçası olarak yapay zeka kullanımı hakkında genel olarak bilgilendirmekle yükümlü kılınabilir.

Müşteri, ayrıca talep üzerine, hizmetlerde yapay zeka kullanımına ilişkin belirli bilgiler alma hakkını talep edebilir. Bir hizmet sağlayıcı, bu tür bir hakkı dengelemek amacıyla ticari olarak hassas iş bilgilerini ve yapay zeka aracını eğitmek için kullanılan veri kümelerine sahip diğer müşterilerin gizli bilgilerini korumak isteyebilir.

PART 21

If a party detects issues with the use or output of AI, then each party will likely seek a mutual obligation to be promptly notified. Key points of negotiation may include the scope of "issues" such as data breaches, inaccurate, biased, or unrepresentative outputs; time period and scope of notification; and consequences of any issues: a remediation plan or suspension right for the use of AI or the services as a whole.

The customer may also have an acceptable AI use policy for its supply chain to which it may require the service provider/supplier to adhere.

C. Accuracy and Reliability Issues

The risk of overreliance on technology is not a 'new' risk – but it is arguably more acute with AI, given the lack of transparency, explainability and auditability of certain types of AI. As with any software-based solution, AI poses risks if it does not produce accurate, reliable results. Thus, before relying on AI tools, businesses will want to know, for example, whether the original data on which the AI was trained was itself reliable, whether there have been any independent evaluations of the tool's reliability and accuracy, the extent to which there will be a "human in the loop" to check for anomalous outputs, the extent to which the service provider or a supplier is prepared to accept liability for errors caused by AI and what remedies it will offer if outputs are wrong.

To address these issues, customers will need to build into the contract sufficient information-provision, testing and audit requirements to ensure that the AI used in the provision of the services, at least to the extent that it is interacting with, or impacting, humans or making important decisions, is explainable.

Where services utilize AI, customers may also expect service providers to ensure that a provider's use of AI will not degrade the contractual standard for performance of the services; produces accurate and representative outputs and does not take into consideration certain protected characteristics, unless the customer has provided preapproval; and does not develop harmful or inappropriate behaviors.

Bir taraf, yapay zeka kullanımı veya çıktılarıyla ilgili bir sorun tespit ederse, her iki taraf da genellikle birbirini derhal bilgilendirme yükümlülüğü talep edecektir. Müzakere edilecek ana noktalar arasında "sorunların" kapsamı (veri ihlalleri, yanlış, önyargılı veya temsil edici olmayan çıktılar gibi), bildirim süresi ve kapsamı ile sorunların sonuçları (yapay zeka kullanımına veya hizmetlerin tamamına yönelik bir iyileştirme planı veya askıya alma hakkı) yer alabilir.

Müşteri ayrıca tedarik zinciri için kabul edilebilir bir yapay zeka kullanım politikası geliştirmiş olabilir ve bu politikaya uyulmasını hizmet sağlayıcıdan/ tedarikçiden talep edebilir.

C. Doğruluk ve Güvenilirlik Sorunları

Teknolojiye aşırı güvenme riski 'yeni' bir risk değildir, ancak yapay zekada bu risk, bazı yapay zeka türlerinin şeffaf olmaması, açıklanabilir olmaması ve denetlenebilir olmaması nedeniyle tartışmasız daha akuttur. Herhangi bir yazılım tabanlı çözümde olduğu gibi, yapay zeka, doğru ve güvenilir sonuçlar üretmezse riskler yaratır. Bu nedenle, işletmeler yapay zeka araçlarına güvenmeden önce, örneğin yapay zekanın eğitildiği orijinal verilerin güvenilir olup olmadığını, aracın güvenilirliği ve doğruluğu konusunda herhangi bir bağımsız değerlendirme olup olmadığını, olağandışı çıktıları kontrol etmek için bir "insan döngüsünün" dahil edilip edilmediğini, hizmet sağlayıcının veya tedarikçinin yapay zekanın neden olduğu hatalardan sorumluluk kabul etmeye ne kadar hazır olduğunu ve yanlış çıktılar olduğunda hangi çözümleri sunacağını bilmek isteyecektir.

Bu sorunları ele almak için, müşteriler, yapay zekanın hizmet sağlama sürecinde kullanıldığını, en azından insanlarla etkileşime geçtiği veya önemli kararlar verdiği ölçüde, açıklanabilir olmasını sağlamak amacıyla sözleşmeye yeterli bilgi sağlama, test ve denetim yükümlülükleri eklemelidir.

Hizmetlerde yapay zeka kullanıldığında müşteriler; sağlayıcıların yapay zeka kullanımının, hizmetlerin sözleşmesel performans standardını düşürmemesini, doğru ve temsil edici çıktılar üretmesini, müşteri önceden onay vermedikçe korunan özel nitelikteki verileri dikkate almamasını, zararlı veya uygunsuz davranışlar geliştirmemesini, ve hizmet sağlayıcıların bu taahhütlerde bulunmasını bekleyebilirler.

The extent to which a service provider is able to meet these expectations will depend on various factors, including how the applicable AI tool is procured and how it is trained on data sets. For example, if such data sets are provided by the customer, then a service provider may seek to carve out errors or inaccuracies in the training data sets from its responsibility.

Some technical standards may be helpful in providing some degree of comfort that the supplier's approach to AI is sufficiently robust. However, it is important to note that when a supplier says it is "compliant" with a particular standard, this is not the same as saying that it has been through a full certification process. Certification requires auditing by an independent third party, which involves a rigorous procedure and can be quite a lengthy and expensive process. "Compliant" means that the supplier adheres to the relevant standard and whilst this can be evidenced (perhaps confusingly) by a "certificate of compliance", the latter relies on internal audits and self-assessments. So, whilst compliance offers some degree of assurance, much depends on how much you trust the supplier to have been rigorous in its own self-assessment.

D. Compliance with Laws

Given the wide range layers of regulations concerning AI such as protection of corporate and personal data, product liability, e-commerce rules, or even attorney client privilege, as the case may be, the contractual allocation of compliance responsibility within the AI ecosystem is becoming increasingly important. Broadly, responsibility for ensuring an AI tool does not violate applicable laws may fall on the party providing the dataset(s) that train the AI tool. A key negotiation point may be whether it is the service provider's responsibility to not cause the customer itself to violate applicable laws through its use of the AI tool, or whether the customer alone is responsible for its own compliance obligations (e.g., sector-specific regulations).

Further, if an AI tool is used to collect or process personal information, then it is crucial to ensure that this data is handled in accordance with relevant privacy laws and regulations. There are ways to potentially navigate risks through anonymization and de-identification, the use of privacy policies, and con-

Bir hizmet sağlayıcının bu beklentileri ne kadar karşılayabileceği, ilgili yapay zeka aracının nasıl edinildiği ve hangi veri kümeleri üzerinde eğitildiği gibi çeşitli faktörlere bağlıdır. Örneğin, bu tür veri kümeleri müşteri tarafından sağlanıyorsa, bir hizmet sağlayıcı, eğitim veri kümelerindeki hatalar veya yanlışlıklar nedeniyle sorumluluktan kaçınmak isteyebilir.

Bazı teknik standartlar, tedarikçinin yapay zekaya yaklaşımının yeterince sağlam olduğuna dair bir güvence sağlamak açısından yardımcı olabilir. Ancak, bir tedarikçinin belirli bir standartla "uyumlu" olduğunu söylemesi, tam bir sertifikasyon sürecinden geçtiği anlamına gelmez. Sertifikasyon, bağımsız bir üçüncü tarafça denetimi gerektirir ve bu, titiz bir prosedürdür ve oldukça uzun ve pahalı bir süreç olabilir. "Uyumlu" terimi, tedarikçinin ilgili standarda uyduğunu ifade eder ve bu durum (belki kafa karıştırıcı bir şekilde) bir "uyum sertifikası" ile belgelendirilebilir; ancak bu, iç denetimler ve öz değerlendirmelere dayanır. Dolayısıyla, uyumluluk bir güvence sağlasa da tedarikçinin kendi öz değerlendirmesinde ne kadar titiz olduğuna güvenip güvenmediğiniz çok önemlidir.

D. Yasalarla Uyum

Yapay zeka ile ilgili kurumsal ve kişisel verilerin korunması, ürün sorumluluğu, e-ticaret kuralları veya avukat-müvekkil gizliliği gibi çok katmanlı düzenlemeler göz önüne alındığında, yapay zeka ekosisteminde uyum sorumluluğunun sözleşmesel olarak dağılımı giderek daha önemli hale gelmektedir. Genel olarak, bir yapay zeka aracının ilgili yasaları ihlal etmemesini sağlama sorumluluğu, yapay zeka aracını eğiten veri setlerini sağlayan tarafa düşebilir. Önemli bir müzakere noktası, müşterinin yapay zeka kullanımı sonucunda herhangi bir yasayı ihlal etmesinden doğan sorumluluğun kime ait olacağıdır: Hizmet sağlayıcı, müşterinin yapay zeka kullanımı nedeniyle herhangi bir yasayı ihlal etmesine sebep olmayacağını taahhüt edecek midir? Müşteri, yapay zeka aracını kullanması nedeniyle doğrudan kendisi mi sorumlu olmalıdır, yasalara uyum (örneğin, sektöre özgü düzenlemelere uyum) yalnızca müşterinin yükümlülüğü müdür?

Öte yandan, bir yapay zeka aracı kişisel bilgileri toplamak veya işlemek için kullanılıyorsa, bu verilerin tabi olunan verilerin korunması

PART 21

tractual provisions; however, close attention should be paid to whether AI has the right to use data in an AI system and how the system uses and discloses information.

E. Ownership and Licensing of Intellectual Property Rights

The top-of-mind issue arising in connection with ownership and use rights when leveraging GenAI is the ownership of intellectual property rights in the layers of input to the AI and the outputs generated from the AI tools. The ability of a company to demonstrate chain of title to input and output is critical for a number of reasons, including in situations where a company wants to sell a product, asset, or potentially its business. Each party will expect the other to stand behind the intellectual property rights that it contributes, typically through indemnification against third-party claims of intellectual property infringement. This tension is the focus of much negotiation in the current AI intellectual property allocation landscape.

If, however, the underlying concern is the ability to use the outputs without any restriction, then this could be achieved through licensing terms. It is also important from both a legal and practical perspective to consider licensing arrangements in the event of a termination of use of the AI tool, whether planned or sudden, in order to minimize service disruption. As ever, it is crucial to prepare for the end of the relationship right at the beginning of it. On exit, there will be similar "lock-in" risks to those that apply for other proprietary software tools - the service provider may be unwilling to provide information or license its AI tool to a replacement provider – but there may be additional issues with data migration to consider in this context as well. It may not be possible to provide training data (e.g. belonging to third parties) to a replacement provider, nor to extract customer data that is held in a data lake. It will be important to mitigate these issues in the contract.

Furthermore, a clause will need to be included on usage restrictions and other license

yasalarına uygun olarak ele alınmasını sağlamak son derece önemlidir. Risk yönetimi yapmanın anonimleştirme ve kimliksizleştirme, gizlilik politikalarının uygulanması ya da spesifik sözleşme hükümleri gibi pek çok yolu bulunmaktaysa da; yapay zekanın bir yapay zeka sisteminde veri kullanma hakkına sahip olup olmadığına, sistemin bilgileri nasıl kullandığına ve ifşa ettiğine çok dikkat edilmelidir.

E. Fikri Mülkiyet Haklarının Sahipliği ve Lisanslanması

Üretken yapay zeka kullanılırken karşılaşılan en önemli konulardan biri, yapay zekaya sağlanan girdilerde ve yapay zeka araçları tarafından üretilen çıktılarda fikri mülkiyet haklarının sahipliğidir. Bir şirketin hem girdilerde hem de çıktılarda mülkiyet zincirini kanıtlayabilmesi, özellikle bir ürün, varlık ya da işletmeyi satmak istediği durumlarda kritik bir öneme sahiptir. Taraflardan her biri diğerinin, genellikle üçüncü tarafların fikri mülkiyet ihlali iddialarına karşı tazminat ödemek yoluyla, katkıda bulunduğu fikri mülkiyet haklarının arkasında durmasını bekleyecektir. Yapay zekanın fikri mülkiyetinin kime ait olduğu ve fikri milkiyet haklarının taraflar arasında nasıl paylaşılacağı konusu, yapay zeka sözleşme müzakerelerinin odak noktasıdır.

Ancak, temel kaygı çıktıları herhangi bir kısıtlama olmaksızın kullanabilmek ise, bu kaygı lisanslama ile giderilebilir. Lisanslama düzenlemeleri, hem hukuken hem de pratikte, yapay zeka aracının kullanımının (planlı ya da aniden) sona ermesi durumunda, hizmet kesintilerini en aza indirmek bakımından da son derece önemlidir. Herhangi bir ilişkide olduğu gibi, bu hukuki ilişkinin sonuna da daha en başından hazırlık yapılmalıdır. Ayrılma aşamasında, diğer tescilli yazılım araçları için geçerli olan lisans sahibine "mahkum kalma" riskine benzer şekilde, hizmet sağlayıcı, yerini alacak sağlayıcıya yapay zeka aracına ilişkin bilgi sağlamayı ya da lisans vermeyi reddedebilir. Ayrıca, bu bağlamda veri göçü ile ilgili ek sorunlar da ortaya çıkabilir. Eğitim verilerinin, örneğin üçüncü şahıslara ait olanların yeni sağlayıcıya aktarılması ya da veri havuzunda tutulan müşteri verilerinin ayıklanması mümkün olmayabilir. Bu sorunların sözleşme içinde giderilmesi önemlidir.

Buna ek olarak, yapay zeka aracının kendisinin ya da üretilen çıktının kullanım kısıtla-

terms of the AI tool itself or of the generated output. The supplier may want to limit the use of generated output to internal use only (and thus prohibit any further commercialisation).

F. Data Sources to Train Large Language Models

The negotiation of GenAI agreements demands a meticulous examination of data sources used to train LLM and generate output. This scrutiny is essential to prevent future practical and legal complications. A comprehensive legal review should assess whether collected data adheres to legal requirements for machine-learning purposes. This assessment requires a deep dive into the company's existing terms of service, privacy policy statements, and other customer-facing contractual terms to ascertain the permissions obtained from customers or users. Different types of data raise distinct consent and liability issues. Personal identifiable information, synthetic content generated by other AI systems, and third-party intellectual property all require careful evaluation.

To proactively address these concerns, many providers implement data minimization, utilizing only necessary data, and transparently explain how LLMs use data for training. This transparency promotes trust and minimizes potential legal challenges.

Service providers can enhance their offerings by training AI on aggregated customer data. However, customers are understandably hesitant to share commercially sensitive information that could benefit competitors. Confidentiality, data protection, intellectual property rights, information security, and post-termination provisions warrant close examination to ensure adequate safeguards for customer data.

Further complexities arise when determining ownership of AI improvements stemming from training data. Various approaches exist, ranging from complete data segregation, where customers own all rights to improvements, to "AI as a service" models where the customer contributes to a shared data pool and the service provider retains ownership of the AI and improvements. Hybrid approaches, striking a balance between customer data protection and service provider innovation, can also be explored.

malarına ve diğer lisans koşullarına ilişkin ayrı bir düzenlemeye ihtiyaç olacaktır. Tedarikçi, üretilen çıktının sadece dahili kullanım ile sınırlandırılmasını ve herhangi bir ticari kullanımın yasaklanmasını isteyebilir.

F. Büyük Dil Modellerini Eğitmek İçin Veri Kaynakları

Üretken yapay zeka anlaşmalarının müzakeresi, Büyük Dil Modellerini (LLM) eğitmek ve çıktı üretmek için kullanılan veri kaynaklarının titizlikle incelenmesini gerektirir. Bu titiz inceleme, gelecekte ortaya çıkabilecek hukuki ve pratik sorunları önlemek için şarttır. Kapsamlı bir hukuki inceleme, toplanan verilerin makine öğrenimi amaçlarına yönelik yasal gerekliliklere uyup uymadığını değerlendirmelidir. Bu değerlendirme, şirketin mevcut hizmet şartları, gizlilik politikası ve müşteri odaklı diğer sözleşme şartlarının derinlemesine incelenmesini ve müşterilerden ya da kullanıcılardan alınan izinlerin doğrulanmasını gerektirir. Farklı veri türleri, farklı onay ve sorumluluk sorunlarını ortaya çıkarır. Kişisel olarak tanımlanabilir bilgiler, diğer yapay zeka sistemleri tarafından üretilen sentetik içerikler ve üçüncü şahıslara ait fikri mülkiyet hakları dikkatle değerlendirilmelidir.

Bu sorunları proaktif olarak ele almak için birçok sağlayıcı, yalnızca gerekli verileri kullanarak veri minimizasyonu uygular ve LLM'lerin verileri eğitim için nasıl kullandığını şeffaf bir şekilde açıklar. Bu şeffaflık, güven tesis eder ve potansiyel yasal zorlukları en aza indirir.

Hizmet sağlayıcılar, yapay zekayı toplu müşteri verileri üzerinde eğiterek tekliflerini geliştirebilir. Ancak, müşteriler haklı olarak, rakiplerine fayda sağlayabilecek ticari açıdan hassas bilgileri paylaşmakta tereddür ederler. Gizlilik, verilerin korunması, fikri mülkiyet hakları, bilgi güvenliği ve hizmetin sona ermesi sonrasına ilişkin hükümler, müşteri verilerinin uygun ölçüde korunmasını sağlayacak güvencelerdir ve dikkatle ele alınması gerekir.

Eğitim verilerinden kaynaklanan yapay zeka geliştirmelerinin sahipliğini belirlemek de ek zorluklar yaratır. Bu konuda, müşterilerin tüm geliştirmeler üzerinde hak sahibi olduğu mutlak veri ayrıştırmasından müşterinin paylaşılan bir veri havuzuna katkıda bulunduğu, hizmet sağlayıcının, yapay zekanın ve geliştirmelerinin mülkiyetini elinde tuttuğu "hizmet olarak yapay zeka" modellerine kadar çeşitli

PART 21

Developers and providers must exercise caution when using copyrighted content for model training. Infringing third-party intellectual property rights in training data risks output infringement if the output substantially copies the training data. Licensing emerges as the best strategy to mitigate copyright infringement claims. To address concerns, some developers offer to defend customers against copyright infringement claims arising from their AI assistant's outputs. Such intellectual property protections could become an industry standard, fostering confidence and reducing legal risk.

These considerations significantly impact the potential liability of suppliers, providers, and developers, influencing their negotiation strategies for indemnification, representations, and warranties in contracts. Customers will demand clarification on training data sources and seek contractual protection against third-party infringement claims. This could include warranties ensuring that AI training processes and outputs do not infringe third-party intellectual property rights or, alternatively, the implementation of technical measures or tools to minimize infringement risks.

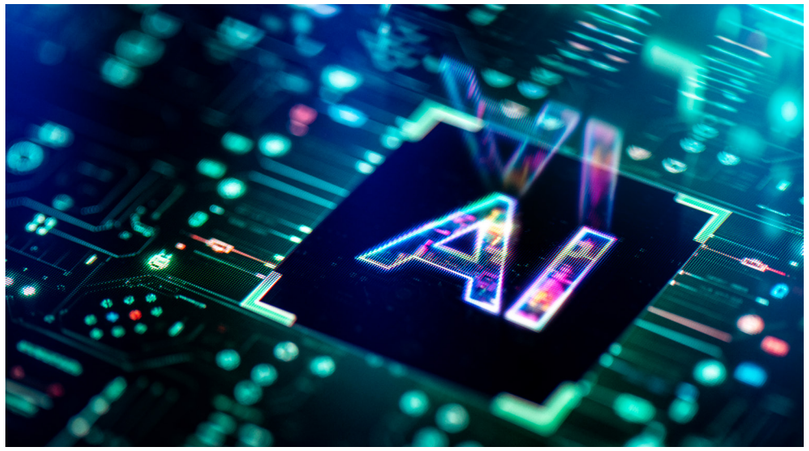
Finally, when AI interacts with third-party software tools, customers should verify that third-party licenses support such use. For example, if licenses are based on human users, additional licenses might be required for AI utilization. This verification safeguards against potential legal disputes and ensures compliance with licensing agreements.

yaklaşımlar mevcuttur. Müşteri veri koruması ile hizmet sağlayıcı inovasyonu arasında denge sağlayan hibrit yaklaşımlar da benimsenebilmektedir.

Geliştiriciler ve sağlayıcılar, modellerin eğitimi için telif hakkıyla korunan içerik kullanırken dikkatli olmalıdır. Eğitim verilerinde üçüncü taraf fikri mülkiyet haklarını ihlal etmek, çıktıların eğitim verilerini önemli ölçüde kopyalaması durumunda ihlal riskini artırır. Lisanslama, telif hakkı ihlal iddialarını azaltmanın en iyi stratejisi olarak görünmektedir. Benzer kaygılara karşı bazı geliştiriciler, müşterilerini yapay zeka asistanlarının çıktılarından kaynaklanan telif hakkı ihlal iddialarına karşı savunmayı teklif eder. Bu tür fikri mülkiyet korumaları, güveni artırarak yasal riski azaltabilir ve endüstri standardı haline gelebilir.

Bu hususlar, tedarikçilerin, sağlayıcıların ve geliştiricilerin olası sorumluluklarını önemli ölçüde etkiler ve tazminat, beyan ve garantilerle ilgili müzakere stratejilerini şekillendirir. Müşteriler, eğitim veri kaynaklarının netleştirilmesini ve üçüncü taraf ihlal iddialarına karşı sözleşmesel koruma talep edecektir. Bu, yapay zeka eğitim süreçlerinin ve çıktılarının üçüncü taraf fikri mülkiyet haklarını ihlal etmediğine dair garantiler ya da ihlal risklerini en aza indiren teknik önlemler veya araçların uygulanmasını içerebilir.

Son olarak, yapay zeka üçüncü taraf yazılım araçlarıyla etkileşime girdiğinde, müşterilerin bu tür kullanımı destekleyen üçüncü taraf lisanslarını doğrulaması gerekir. Örneğin, lisanslar gerçek kullanıcılara dayalıysa, yapay zeka kullanımına yönelik ek lisanslar gerekebilir. Bu doğrulama, olası yasal anlaşmazlıklara karşı koruma sağlar ve lisans sözleşmelerine uygunluğu güvence altına alır.



The negotiation of GenAI agreements is a complex process requiring careful consideration of data sources, intellectual property, and liability issues. By proactively addressing these concerns through transparent practices, robust legal frameworks, and effective contractual provisions, stakeholders can navigate the evolving landscape of GenAI and foster responsible innovation.

G. Liability

As there are many parties involved in an AI system, who will be held liable may be difficult to establish and there are many factors that should be taken into consideration. These factors include whether the AI system was following instructions, whether damage can be traced back to the design or production of the AI system and whether the AI system provided any general or specific limitations. Contributory negligence will also be considered as a factor here.

Negotiating liability provisions in AI contracts requires careful consideration of the unique challenges posed by this technology. While many principles align with those in broader technology and services contracts, AI presents specific risks that warrant dedicated attention. In traditional technology transactions, suppliers often seek to limit their liability for breaches of representations and covenants, such as those related to documentation, quality, or third-party consents. This typically involves capping liability for damages or outlining exclusive remedies like repair, reperformance, or specified credit or liquidated damages payments. However, AI introduces new complexities. One key challenge is the attribution of fault, particularly in scenarios involving human-AI interaction. For example, in the context of robotic surgical assistance, determining responsibility for an adverse event can be complex, raising questions about how to apply contractual provisions to such situations.

AI's potential for widespread application also necessitates consideration of scenarios where bodily injury or harm to individuals is a risk, such as AI-driven medical procedures

Üretken yapay zeka anlaşmalarının müzakeresi, veri kaynakları, fikri mülkiyet ve sorumluluk konularının dikkatlice ele alınmasını gerektiren karmaşık bir süreçtir. Bu endişeleri şeffaf uygulamalar, sağlam hukuki çerçeveler ve etkili sözleşme hükümleri ile proaktif bir şekilde ele alarak, paydaşlar üretken yapay zekanın gelişen dünyasında sorumlu yenilikleri teşvik edebilir.

G. Sorumluluk

Yapay zeka sistemine birçok taraf dahil olduğu için, kimin sorumlu tutulacağının belirlenmesi zor olabilir ve bu hususta dikkate alınması gereken birçok faktör vardır. Bu faktörler arasında yapay zeka sisteminin talimatlara uygun hareket edip etmediği, hasarın yapay zeka sisteminin tasarımına veya üretimine dayandırılıp dayandırılamayacağı ve yapay zeka sisteminin genel veya özel sınırlamalar sunup sunmadığı yer alır. Ayrıca, müşterek kusur da önemli bir diğer faktör olarak değerlendirilecektir.

Yapay zeka sözleşmelerinde sorumluluk hükümlerinin müzakere edilmesi, bu teknolojinin getirdiği benzersiz zorluklar nedeniyle dikkatli bir değerlendirme gerektirir. Daha geniş teknoloji ve hizmet sözleşmelerinde yer alan ilkelerle paralellik gösterse de, yapay zeka sistemleri spesifik riskler sunduğundan daha özellikli bir yaklaşım gerektirir. Geleneksel teknoloji işlemlerinde, tedarikçiler genellikle belgelere, hizmet kalitesine veya üçüncü taraf izinlerine dayanan beyan ve taahhütlerin ihlali durumlarında sorumluluklarını sınırlandırmaya çalışır. Bu hallerde genellikle zararın sınırlandırılması veya onarım, hizmetin yeniden ifa edilmesi veya belirli kredi yüklemesi ya da maktu tazminat ödemesi yollarına başvurulur. Ancak, yapay zeka sistemleri yeni ve karmaşık zorluklar ortaya çıkarmaktadır.

Bu ana zorluklardan biri, özellikle insan-yapay zeka etkileşimi içeren senaryolarda, hatanın nerede olduğunu belirlemektir. Örneğin, robotik cerrahi yardımı bağlamında, olumsuz bir olay meydana geldiğinde sorumluluğun belirlenmesi karmaşık olabilir ve bu tür durumlarda sözleşme hükümlerinin nasıl uygulanacağı sorununu gündeme getirir.

PART 21

or autonomous vehicles. Moreover, AI's ability to fail in systemic yet difficult-to-detect ways presents a unique challenge. Damages could accumulate rapidly before either party realizes an issue exists.

These factors necessitate careful consideration of two crucial contract provisions: disclaimers and limitations on liability. In standard technology contracts, suppliers often disclaim implied warranties and restrict remedies for quality or non-compliance issues. This practice is most likely to extend to AI contracts, with suppliers seeking to ensure customers assume risks associated with AI use, particularly in human-AI interactions or high-risk applications. This could involve contractual obligations for customers to understand AI features, proper use, and inherent risks, and to confirm receipt of related documentation.

Customers, however, should avoid accepting overly broad disclaimers that completely absolve suppliers from liability for AI-caused harm. If customers can secure adequate documentation and quality assurances, they may be able to negotiate exceptions for express warranties. Additionally, customers should ensure that limitations on remedies do not preclude other claims arising from the same transaction and avoid language that restricts remedies when the customer is partially at fault, given their limited AI expertise.

In AI contracts, suppliers' liability limitations will largely mirror those in other technology agreements. However, customers face unique challenges due to the nature of AI. They should avoid limiting suppliers' liability for consequential damages arising from AI law violations, particularly given transparency issues and the limited understanding of AI among most users. Similarly, customers should avoid limiting liability for damages caused by AI suspension due to regulatory actions traceable to the supplier.

While both parties may seek to limit liability based on fault, attributing fault can be complex in human-AI interactions. A third-party neutral or an alternative dispute resolution mechanism could be employed to facilitate fault attribution.

Even with liability exclusions, customers may reasonably expect suppliers to defend against third-party claims, leveraging their superior AI knowledge. An independent fault attribution mechanism can foster collaboration in defense efforts and facilitate equitable cost allocation.

In conclusion, negotiating liability provisions in AI contracts requires a nuanced approach that balances the unique challenges posed by this technology with the need for clear and enforceable contractual terms. By carefully considering the risks inherent in AI, both suppliers and customers can ensure that their agreements adequately protect their interests. However, it is also reasonable to consider limitations of liability in favor of suppliers, given the evolving nature of AI technology. Suppliers may argue that due to the nascent stage of AI development, certain limitations on liability are justified to encourage innovation and investment in AI technologies. This balanced approach ensures that while customers are protected, suppliers are not unduly burdened, allowing for a fair distribution of risks and responsibilities.

Yapay zekanın yaygın kullanım potansiyeli, ayrıca bireylerin yaralanma veya zarar görme riskini taşıyan senaryoları da içerebilir. Yapay zeka destekli tıbbi prosedürler veya otonom araçlar gibi durumlar buna örnek olarak gösterilebilir. Dahası, yapay zekanın sistemik ancak tespiti zor bir şekilde başarısız olabilme potansiyeli, benzersiz bir zorluk yaratır. Taraflardan biri sorunun farkına varmadan önce zarar çoktan ortaya çıkmış ve hızla birikmiş olabilir.

Bu faktörler, sorumluluğun reddi ve sınırlandırılması gibi iki önemli sözleşme hükmünün dikkatle ele alınmasını gerektirir. Standart teknoloji sözleşmelerinde, tedarikçiler genellikle zımni taahhütleri reddeder ve tazmin etme sorumluluklarını kalite veya uyum sorunları ile sınırlandırır. Bu yaklaşım büyük olasılıkla yapay zeka sözleşmelerinde de bencimsenecektir: Tedarikçiler, özellikle insan-yapay zeka etkileşimli veya yüksek riskli uygulamalarda, müşterilerin yapay zeka kullanımıyla ilgili riskleri üstlenmesini sağlamaya çalışacaktır. Bu durum, müşterilerin yapay zeka özelliklerini, bunların doğru kullanımını ve içerdiği riskleri daha iyi anlamalarını gerektirecek ve sözleşmeler müşterilerin yapay zeka kullanım yönergelerini aldıklarını teyit etmelerini gerektiren yükümlülükler içerecektir.

Müşteriler ise, yapay zeka kaynaklı zararlarda tedarikçileri tamamen sorumluluktan kurtaran hükümlerden kaçınmalıdır. Müşteriler yeterli dokümantasyon ve kalite güvencesi sağlayabilirse, sarih taahhütler için istisnalar müzakere edebilirler. Ayrıca, müşteriler, çözüm yollarına ilişkin sınırlamaların aynı işlemden kaynaklanan diğer talepleri engellemediğinden emin olmalı ve sınırlı yapay zeka uzmanlıkları göz önüne alındığında, müşterinin kısmen hatalı olduğu durumlarda çözüm yollarını kısıtlayan dilden kaçınmalıdır.

Yapay zeka sözleşmelerinde tedarikçilerin sorumluluk sınırlandırmaları, büyük ölçüde diğer teknoloji anlaşmalarındakileri yansıtacaktır. Ancak, yapay zekanın doğası gereği müşteriler benzersiz zorluklarla karşılaşır. Müşteriler, özellikle yapay zekaya ilişkin şeffaflık meselesi ve çoğu kullanıcı tarafından sınırlı düzeyde anlaşılabilirliği göz önüne alındığında, yapay zeka yasalarının ihlali nedeniyle ortaya çıkan sonuçsal zararlar için tedarikçilerin sorumluluğunu sınırlandırmaktan kaçınmalıdırlar. Benzer şekilde, müşteriler tedarikçiye atfedilebilecek düzenleyici işlemler nedeniyle yapay zekanın askıya alınmasından kaynaklanan zararlar için sorumluluk sınırlandırmalarından kaçınmalıdır.

Her iki taraf da sorumluluğu kusura dayalı olarak sınırlandırmaya çalışsa da insan-yapay zeka etkileşimlerinde hatanın nereye ait olduğunu belirlemek kolay olmayabilir. Üçüncü bir tarafın tarafsızlığı ya da alternatif bir uyuşmazlık çözüm mekanizması, kusurlu tarafın belirlenmesini kolaylaştırabilir.

Sorumluluktan kurtulma düzenlemelerine rağmen, müşteriler tedarikçilerin, yapay zeka alanında daha fazla bilgi sahibi olma avantajlarını kullanmak üzere, üçüncü taraf iddialarına karşı savunma sağlamasını bekleyebilirler. Kusurlu tarafın kim olduğunu tespit için bağımsız bir kişinin atanması, savunma çabalarında işbirliğini teşvik edebilir ve maliyetin adil bir şekilde paylaşımını sağlayabilir.

Sonuç olarak, yapay zeka sözleşmelerinde sorumluluk hükümlerinin müzakere edilmesi, bu teknolojinin sunduğu benzersiz zorlukları açık ve uygulanabilir sözleşme koşulları ile dengeleyen hassas bir yaklaşım gerektirir. Yapay zekanın içerdiği riskler dikkatle değerlendirildiğinde hem tedarikçiler hem de müşteriler, anlaşmalarının çıkarlarını yeterince koruduğundan emin olabilirler. Bununla birlikte, yapay zeka teknolojisinin gelişen doğası göz önüne alındığında, tedarikçiler lehine sorumluluk sınırlamalarını dikkate almak da makul sayılabilir. Tedarikçiler, yapay zekanın gelişmekte olan bir teknoloji olduğu

PART 21

III. USE OF AI TOOLS TO DEVELOP SOFTWARE

The legal implications of AI contracting can be especially complex when a supplier utilizes AI tools not to directly provide AI services, but to develop software that is subsequently delivered to customers. In such scenarios, the contractual terms governing the AI tool become paramount, as the supplier might be reluctant to make guarantees to its customer that extend beyond those terms. For instance, if the AI tool provider does not offer indemnification for third-party intellectual property infringement arising from the generated output, the supplier may be similarly unwilling to provide such assurance to its customer. Conversely, even with an indemnification clause in the AI tool contract, the extent to which it applies to modifications made by the supplier during software development remains a question.

Similarly, the ownership of the generated output can pose challenges. If the AI tool disclaims ownership of generated output without guaranteeing non-infringement of third-party intellectual property rights, the supplier's contract with the customer may lack similar warranties, potentially leaving the ownership of the final software unclear.

Finally, the use of open-source software by AI-powered development processes further complicates matters. Typically, suppliers can control the use of open-source software in software development, mitigating copyleft license risks. However, when an AI tool operates as a "black box" - where training processes and data are obscured from the user - it becomes difficult for the supplier to offer similar assurances regarding open-source software usage.

gerekçesiyle, yapay zeka teknolojilerinde yeniliği ve yatırımı teşvik etmek için sorumluluk sınırlamalarının haklı olduğunu savunabilir. Bu dengeli yaklaşım, müşteriler korunurken tedarikçilere gereksiz yük getirilmemesini sağlayarak risk ve sorumlulukların adil bir şekilde dağıtılmasına olanak tanır.

III. YAPAY ZEKA ARAÇLARININ YAZILIM GELİŞTİRME İÇİN KULLANILMASI

Yapay zeka sözleşmelerinin ortaya koyacağı hukuki meseleler, özellikle tedarikçi yapay zeka araçlarını doğrudan yapay zeka hizmetleri sağlamak için değil, daha sonra müşterilerine teslim edeceği yazılımları geliştirmek için kullandığında daha da karmaşık hale gelebilir. Bu senaryoda, tedarikçi müşterisine sözleşme hükümlerinin ötesine geçen taahhütlerde bulunmak istemeyeceğinden, sözleşme düzenlemeleri çok daha önemli hale gelir. Örneğin, yapay zeka aracı sağlayıcısı, üretilen çıktıdan kaynaklanan üçüncü taraf fikri mülkiyet ihlali için tazminat ödeme taahhüdünde bulunmazsa, tedarikçi de müşterisine bu tür bir güvence sağlamak istemeyecektir. Diğer taraftan, yapay zeka aracı sözleşmesinde bir tazminat taahhüdü olsa bile, bu taahhüdün yazılım geliştirme sırasında tedarikçi tarafından yapılan değişikliklere ne ölçüde uygulanacağı bir soru olmaya devam etmektedir.

Benzer şekilde, üretilen çıktının mülkiyeti konusunda da bazı zorluklar ortaya çıkabilir. Yapay zeka aracı sağlayıcısının üretilen çıktı üzerinde mülkiyet iddiası olmadığı ve üçüncü taraf fikri mülkiyet haklarının ihlal edilmediğine dair herhangi bir taahhütte bulunmadığı düzenlenmişse, tedarikçinin müşterisiyle yaptığı sözleşmede de benzer düzenlemeler olabilir ve bu da nihai yazılımın mülkiyetini belirsiz hale getirebilir.

Son olarak, yapay zeka destekli geliştirme süreçlerinde açık kaynaklı yazılım kullanımına yönelik sorunlar da konuyu daha da karmaşıklaştırmaktadır. Genellikle, tedarikçiler yazılım geliştirmede açık kaynaklı yazılımların kullanımını kontrol ederek copyleft lisans risklerini yönetebilir. Ancak, bir yapay zeka aracı "kara kutu" olarak çalıştığında, yani eğitim süreçleri ve veriler kullanıcıdan gizlendiğinde, tedarikçinin açık kaynak yazılım kullanımıyla ilgili benzer güvenceler sunması zorlaşır.

IV. CONCLUSION

In conclusion, the intricate task of balancing a company's need for improved quality checks with the goal of achieving cost savings through GenAI solutions presents a notable challenge. Nevertheless, these obstacles can be addressed with advanced technology and meticulous human supervision. GenAI applications, from predictive analytics to virtual assistants, are revolutionizing traditional software contract models, offering unique opportunities while also introducing new legal challenges.

The emergence of AI contracts brings numerous contractual issues, particularly in the realm of intellectual property. This necessitates that both suppliers and customers thoroughly review their existing standard software contracts and devise innovative, unconventional solutions, requiring compromises from both parties. It is evident that adopting an AI-centric approach is crucial for both suppliers and customers to fully capitalize on the benefits of AI contracting.

AI tools can significantly impact outsourcing and other service contracts, promising substantial gains in cost, time, accuracy, scalability, and productivity, benefiting both negotiating parties. To harness these advantages, it is essential to remain vigilant about the "new" risks associated with AI usage in these arrangements. As discussed in this briefing, some of these risks may be entirely new, while many are reconfigurations of familiar challenges. As AI technology continues to evolve rapidly, and the full extent of its risks remains uncertain, there are established contractual mechanisms in service contracts that parties can employ and develop now to mitigate known risks and incorporate flexibility for yet-to-be-understood risks. Businesses should aim to proactively address these issues.

IV. SONUÇ

Sonuç olarak, şirketlerin daha gelişmiş kalite kontrollerine olan ihtiyaçları ile üretken yapay zeka çözümleri aracılığıyla maliyet tasarruflarını artırma hedefleri arasında bir denge kurma, karmaşık fakat dikkate değer bir iştir. Ancak, bu zorlu iş, ileri teknoloji ve titiz insan denetimiyle ele alınabilir. Tahmine dayalı analitikten sanal asistanlara kadar üretken yapay zeka uygulamaları, geleneksel yazılım sözleşmesi modellerinde devrim yaratmakta, benzersiz fırsatlar sunarken yeni yasal zorluklar da ortaya çıkarmaktadır.

Yapay zeka sözleşmelerinin ortaya çıkışı, özellikle fikri mülkiyet alanında birçok sözleşmesel mesele doğurmaktadır. Bu durum hem tedarikçilerin hem de müşterilerin mevcut standart yazılım sözleşmelerini kapsamlı bir şekilde gözden geçirmesini ve her iki tarafın da bazı ödünler vermesini zorunlu kılan yenilikçi, alışılmadık çözümler üretmesini gerektirir. Yapay zeka merkezli bir yaklaşımın benimsenmesinin hem tedarikçilerin hem de müşterilerin yapay zeka sözleşmelerinin sunduğu avantajlardan tam olarak yararlanabilmeleri için hayati önem taşıdığı açıktır.

Yapay zeka araçları, hizmetlerin dış kaynaklardan edinilmesine ilişkin sözleşmeleri (taşeron sözleşmeleri) ve diğer hizmet sözleşmelerini önemli ölçüde etkileyebilir ve her iki müzakere tarafına da maliyet, zaman, doğruluk, ölçeklenebilirlik ve üretkenlik açısından büyük kazanımlar vaat edebilir. Bu avantajlardan yararlanmak için, sözleşmesel düzenlemelerde yapay zeka kullanımına ilişkin "yeni" risklere karşı dikkatli olmak esastır. Makalemizde tartışıldığı gibi, bu risklerin bazıları tamamiyle yeni olabilirken, birçoğu tanıdık zorlukların konfigüre edilmiş halleridir. Yapay zeka teknolojisi hızla gelişmeye devam ettiğinden ve risklerin tam kapsamı belirsizliğini koruduğundan, hizmet sözleşmelerinde tarafların bilinen riskleri azaltmak ve henüz anlaşılmamış riskler için esneklik sağlamak için kullanabilecekleri ve geliştirebilecekleri yerleşik sözleşme mekanizmaları vardır. Şirketler bu konuları proaktif olarak ele almayı hedeflemelidir.